International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 2, June-August, 2017 | Pages 11-23

# STEGANOPIN: A PIN ENTRY METHOD with SHOULDER SURFING RESISTANCE

**C.Ganesh[1], D.Ashok[2]**

[1]Department of Computer Science and Engineering, SRM University, India
[2]Assistant Professor, Department of Computer Science and Engineering, SRM University, India

**Abstract**

Automated Teller Machine (ATM) frauds are escalating gradually. The principal cause for this is the repetition of same personalized identification numbers (PINs) for multiple systems or accounts. Indirect PIN entry methods though available are not yet deployed everywhere and are not user friendly. To increase security and applicability we have implemented a new PIN entry method called SteganoPIN. The interface consists of two keypads, one, a regular sized ATM keypad and the other, a smaller covered keypad. This will help in preventing shoulder surfing attacks. We have proposed another method for PIN entry called Session key technique. The layout of this method comprises a vertical list of digits( 0 to 9), collocated with another list of ten familiar symbols such as = and % etc. Here, the users use symbols instead of numbers and is therefore very secure.

**Keywords:** E-voucher, Personalized identification number (PIN) entry, Shoulder surfing attacks, Steganography, Virtual Money

## 1. Introduction

Personal Identification Numbers are those numbers which are exclusively constructed for the purpose of unlocking and authentication of user, in particular in association with an ATM Card. They are also used for locking and unlocking of doors and smart phones. They are usually made up of numbers which are used as passwords by the users. Convenient usage of these numbers due to modern touch screens has increased their usage and they are implemented on different machines and devices such as point-of-sale (POS) terminals, debit card terminals, digital door-locks, smart phones and tablet computers.

Such a convenient technique doesn't come without flaws. When the secret PIN is entered into such systems, especially in public places, shoulder-surfing is possible. It is one of the direct observation techniques where a third person can obtain the PIN by simply looking over the user's shoulder. This human-only shoulder surfing attacker doesn't cause any serious danger and is considered a weak adversary as he uses only manual tools and suffers from lack of external devices. However, the camera- based shoulder surfing attacker who is equipped with devices such as a wearable camera, that records the whole transaction, can be dangerous.

Impersonation of user is also possible when the attacker has already mounted several shoulder-surfing attacks. Another type of attacker is the Active-guessing attacker. This type of attack is focused on guessing the user's PIN which can be enhanced through repeated camera-based observation of the same user and system. Observation from places other than the ATMs is also possible. The attacker can install high-resolution cameras in public places to monitor the user. Repeated camera-based shoulder surfing attacks pose a realistic threat to the PIN user interface.

Thermal camera-based attacks are increasing recently. A video on the internet went viral when a man explained how a simple iphone case can be used in order to capture the thermal images of a keypad. At the end of the video the man has also given precautionary measures to prevent this type of attack. The idea behind this attack is when the user's body heat gets transmitted on the keypad upon contact the keys radiate different colors in the thermal image. The last pressed key has a strong red color whereas the most faded out color seems to be the first digit of the user's PIN.

Generally, users tend to keep the same PIN for multiple systems. Thus, if an attacker finds out the PIN of the user, he can breach multiple systems. The PIN must be kept sufficiently large so that information is not leaked even under circumstances like repeated observation. Upon knowing the PIN, the attackers can even pick pocket the user's ATM card and gain access to his bank account.

### 1.1. Background and Related Work

To prevent shoulder surfing, various methods have been proposed in the past. These methods were focused on improving security against attackers during the PIN entry time. Indirect PIN entry methods where the visible keypad is hidden or a new keypad is used were proposed. Biometric authentication, e.g., by fingerprint, offers a promising alternative from a usability standpoint, but remains extremely vulnerable to specific observation attacks. Biometric information can easily be captured by using duplicate banking terminals, in a manner similar to capturing access codes and credit card numbers, which in turn can be used to access the users' account.

#### 1.1.1 Color PIN

Roth et al proposed a PIN input system where the input is given indirectly to the system, concealing the original PIN. In the PIN input panel, half of the numbers are black in color whereas the other half is in white. Users are then required to select the color that corresponds to the PIN number. Here, an adversary would not be able to find the users' password which makes the system shoulder-surfing resistant. But every system has a flip side. This system is vulnerable to guessing attack as its inputs can be narrowed down to either black or white. The adversary

also has the option of ruling out the numbers that doesn't correspond to the user's input after multiple login sessions.

### 1.1.2 Convex Hull Click

The convex hull click (CHC) was introduced by Wiedenbeck et al in 2006. Here, random images are used for during the authentication session. Out of five images, three images belong to the user's password. A polygon is to be formed by the users mentally and they have to click anywhere inside the polygon. Users need multiple rounds before they can log in to the system successfully. The area inside the convex hell is used as the "target" password for user authentication. This method hides the number of password images used in the challenge set as only one click is needed from the user per challenge set. However, this method has its own disadvantages too. The polygon which is formed using any three of the password images can be used by an adversary for his/her benefit when an attack is to be launched. One would argue that the number of password images be increased for the benefit of the user. But it makes the system more vulnerable as more password images mean that the polygon formed will be a large area and the "Target" Password can be anywhere within this area. Hence, the vulnerability of the system is increased with respect to guessing attack. A few graphical password schemes against observation attacks were proposed by Sobrado and Birget. One typical scheme called CHC (convex hull click) asks the user to click a random point inside a pentagon which is formed by three or more password images. This scheme was later tested in a user study reported by Wiedenbeck et al. A similar scheme called S3PAS was proposed. Two attacks on CHC were recently reported in [4]. In addition, the usability is not encouraging: the average login time is longer than 70 seconds. The user study was performed on a small password space of size 3 C (112, 5) ≈ 227, so the usability will be much worse if the password space has to be enlarged significantly.

### 1.1.3 Graphic Password Authentication

Weinshall introduces an approach where the user’s password is a set of machine generated pictures. The user must remember the pictures in order to log in to his account. The user has to trace a path in his mind that includes the password pictures and must come with the right answer for a multiple choice question. Authentication is possible only if the user completes these challenge-response sets. Since only the user knows which path was traced, any outside person or a robot set up by outsiders cannot find the password of the user. On the other hand, usability is very low which is a disadvantage and everyday authentication is very much limited when using them. Interesting research has also been conducted on various numbers of diverse authentication methods. The best among these was the biometric authentication as evaluated for ATM usage by Coventry et al. While biometry performs rather well on usability and speed, it is difficult to implement them in a practical perspective and they cost more when compared with other approaches.

### 1.1.4 Tactile Feedback

The devices attached to the terminal provide tactile feedback for authentication purposes which is proposed by Sasamoto et al. For example, the ball movement in undercover is only felt by the user holding it. Each movement is decrypted as a different pad layout which is used in defining a password picture within a set of five pictures. One major drawback in this approach is that the additional fixed hardware which is being used can be controlled by the attackers since they are publicly available to everyone.

### 1.1.5 Vibra Pass

To enable secure authentication on public terminals, De luca et al proposed the VibraPass. Here, PINs and Passwords are enriched with 'lies', i.e. useless interactions are introduced with the aim of confusing the observer. in addition to the real password, these useless lies are randomly mixed with them. Only the user is aware about the lies as it is discreetly shared between the terminal and the user. Hence, the real password is extracted from the input by the terminal.

### 1.1.6 Gaze-Based Authentication

A spy-resistant keyboard proposed by Tan et al uses a level of indirection which makes it less likely for the observer to guess the password. The observer is put in a state of ambiguity as he will not be able to find out the user's choice without the layout design of the entire keyboard. Nevertheless, the password can be entered only by using an keyboard layout and complex interaction technique which is alien to the user. Maeder et al presents a user authentication scheme that is gaze-based where the user is presented with an image and can only log in if the previously specified points of interest is performed on the image is the same as the predetermined order. Malicious users can estimate the order of the points of interest on the image. But the authors choose to ignore this flaw in the method. On top of this, traditional passwords are not supported by this technique.

### 1.1.7 Spin Lock

Bianchi et al presents a novel input keypad with the design and implementation capable of composing a password using tactile cues. Here, randomized vibration patterns correspond to specific passwords which show that the selected items cannot be detected by an observer. A system that is based on a repeated display of single, simple and easy to recognize cue instead of a set of structured stimuli is the Spin lock. A discussion is presented between the observed differences between the audio and haptic cues. Kumar et al introduced a system that works by concealing the user input by solely relying on the user's gaze to enter a password. While promising, the approach is quite expensive as it requires high end eye tracking apparatus. In addition, an external eye-tracker set up by a third person near the original device could track

user passwords. The users have the option of changing their finger pressure but the author's own user study demonstrates that it is difficult to use. Lei et al presented a virtual password system which bypasses observation attacks. The system is based on a linear function that acts in a random manner. But this virtual password system does not guarantee security as an equivalent password is possible through several observations.

### 1.1.8 Shield Pin

Kim et al studied various authentication methods to secure numerical and graphical password entry with multi touch inputs on tabletop computers. ShieldPIN proposes a system where the user has to put one hand in a Γ-shape to cover the keypad whereas the other hand is used for entering the PIN on the keypad. When compared to ShieldPIN, in CuePIN the users place one hand in the same shape to use the random keypad and the other hand is used for scrolling the slots for entering the PIN. Users should identify the digit in the challenge keypad that corresponds to the response keypad first, and then enter the PIN the response keypad. The hand-cover shape used in ShieldPIN does not guarantee good security with shoulder-surfers as it is at an open angle and in CuePIN, the standard numeric keypad does not support its slot-based interface and user operations.

## 2. Steganopin System

For multiple authentication sessions, to prevent camera based shoulder surfing attacks this paper presents an indirect PIN entry method called SteganoPIN. To advance security and usability to PIN-based authentication, this system is proposed.

### 2.1 Usability

Should incur limited increases in PIN entry time and error rates. Should use the regular numeric keypad for key entry. Should not increase the length of a long-term PIN.[1]

### 2.2 Strong Security

Should be resistant to camera-based shoulder surfing attacks. Should be resilient to active guessing attacks.[1]

### 2.2 Theory

Steganography is the art of hiding messages or information within other non-secret text or data. Here the One Time PIN OTP) generated using the challenge keypad conceals the real PIN and therefore the name SteganoPIN. For making it user friendly, we have incorporated a unique user interface with two keypads and a human-machine interaction method to make the process secure against adversaries.

### 2.2.1 User Interface

The user interface of SteganoPIN consists of a standard keypad which is in regular layout and the other one, a small separate keypad in random layout. The random layout keypad permutes ten numeric keys as a random challenge, and is called the challenge keypad. This challenge keypad is used to derive a fresh OTP. For every user, a new OTP will be generated. The user first identifies a long-term PIN in the regular keypad and consequently maps the key locations in the challenge keypad. The user then enters the OTP on a regular keypad called the response keypad. If the OTP is forgotten before entry or if the PIN length is greater then the procedure can be repeated. In the two-faced keypad system, users' familiarity with the regular key locations of the long-term PIN can ease the OTP derivation process.

### 2.3.2 Human-Machine Interaction Method

The response keypad appears in its regular layout and size. The SteganoPIN system displays four circles [see Fig.1]. When three out of these four circles are touched i.e when a user cups a hand on the circle with the grip circularly closed in a ρ-shape [see Fig. 2]. The challenge keypad then shows up after a small delay and immediately disappears when the user releases the cupped hand. This procedure along with the small size of the challenge keypad helps to protect it by visually occluding the keypad from adversaries. A touch screen along with proximity sensor can be used for implementation. Both touch and proximity somewhere around the circle are required, and if either of these conditions is released, then the challenge keypad disappears.

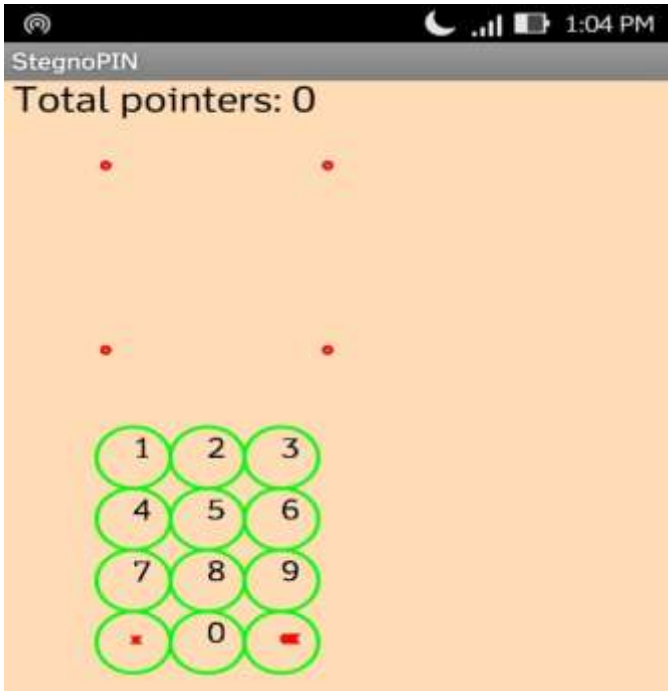


Fig.1

Fig.2

### 2.4 Prototype

We have implemented a prototype system of SteganoPIN to replicate an ATM interface with a smart phone with touch and proximity sensors to implement the response keypad and the challenge keypad. To derive the OTP (One Time PIN) , the user puts a cupped hand touching three out of four point and reads the challenge keypad. The user then enters the OTP in the response keypad. If the PIN length is greater than four digits or if the user forgets part of the OTP then, the user could repeat the procedure. Also, the hand use is made flexible i.e, they can use single or both of their hands for OTP derivation and entry.

## 3. Session Key Method

We propose improved tools to evaluate the resistance of a PIN-entry method. First, we construct a theoretical framework to rigorously define and estimate the security. We also present an example PIN-entry method and show that this method is significantly more secure and usable than previous proposals.

It is a new PIN-entry method. The layout of our method comprises a vertical list of digits(0 to 9), collocated with another list of ten familiar symbols such as = and % etc [see Fig.3]. Additionally, we have three buttons namely, Up, Down and OK. We need four rounds totally,

assuming that the number of digits in a PIN is four, although the method we have proposed can be applied to any case with $N \geq 2$ digits. In the first round, the user has to choose any one of the symbols as their password(which remains constant for the rest of the rounds).The user then, has to align the symbol with the first digit of their PIN using the buttons ("Up" and "Down") [see Fig.4 and 5] and then hit the "OK" button. In the remaining rounds, the user is again given a random list of symbols and s/he rotates the symbol list to align the symbol [previously chosen] with the current PIN digit.

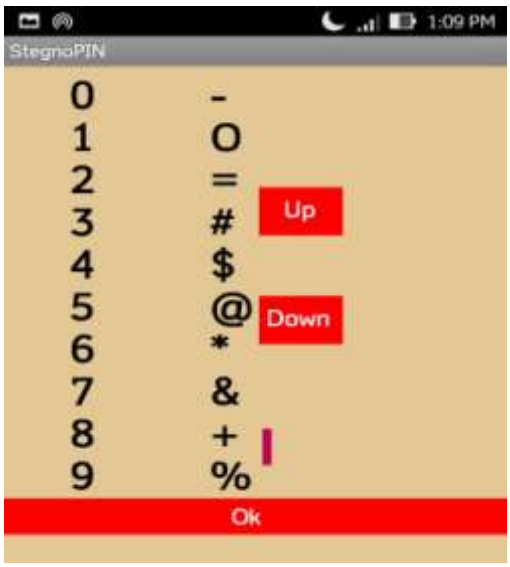


Fig.3

Fig.4

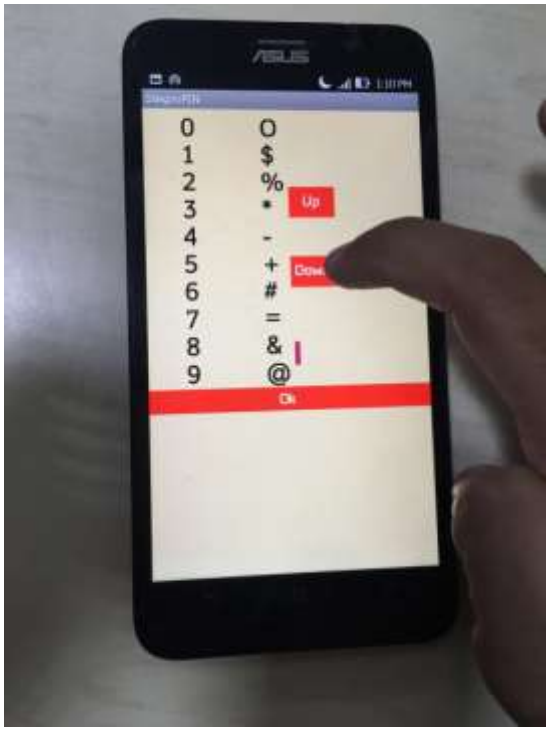
0 O
1 $
2 %
3 *
4 -
5 +
6 #
7 =
8 &
9 @
Up
Down
Ok

Fig.5

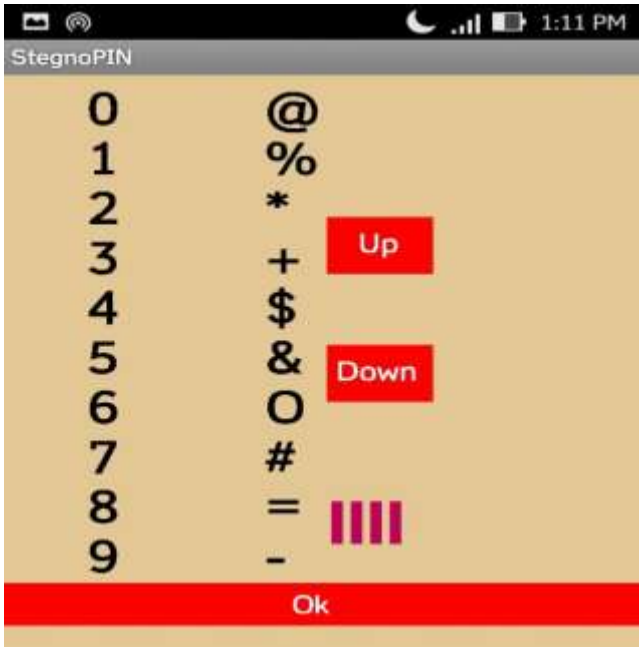
1:11 PM
StegnoPIN
0 @
1 %
2 *
3 +
4 $
5 &
6 O
7 #
8 =
9 -
Up
Down
Ok

Fig.6

For example, let us assume that the PIN is 1234. Now, the user has to choose any one of the symbols as their password. Let us take the user chosen password as "&". The user has to use the "Up" and "Down" buttons to align "&" with the first digit of the PIN i.e 1 and then click OK.

The same procedure needs to be followed to align "&" with the remaining digits of the PIN. Therefore, by using this method, users are not directly entering their personalized identification numbers but, some random symbol thus preventing it from shoulder surfing attacks.

**4. Using Android To Create An ATM Application**

To enhance security and privacy, the ATM application is been moved to the smart phones. Now-a-days, smart phones are used by everyone and it has become a basic need. We have created an ATM application using android where the user first, registers into the application. Basic details such as username, password, email id ,phone number etc need to be filled to complete the registration process.

An optional mobile number is also queried to which a SMS will be sent, if a user or an intruder enters the wrong password more than three times, during the login process and the account will be blocked. Once the registration process is completed, a unique PIN is sent to the respective email id of the user. Then, the user can login into the application with their user name and password. The user is given two options(SteganoPIN or Session Key) for PIN entry. Any one of the method may be selected for entering the PIN. After the user's PIN is validated, the ATM transactions can be performed by the user by using the application.

**4.1 E-Voucher**

Virtual money is commonly termed as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community"[2].E-voucher comes to a person's rescue when he/she is out of cash or doesn't have credit/debit cards.

The user can create a voucher using the ATM application for a specified amount, which is represented using tokens or an image. Every voucher will have a unique voucher id. This process is similar to the Sodexo passes issued by various companies. It can be used to make payments in a secure and easy way.

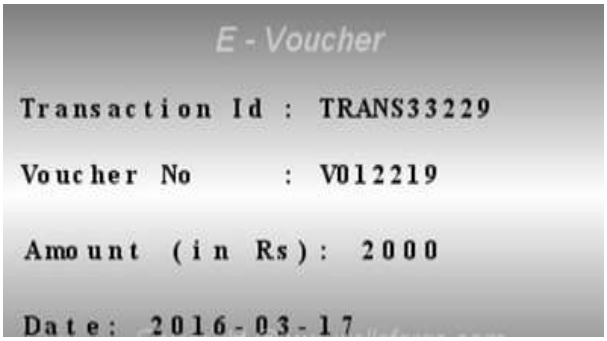


Fig.7

## 5. Architecture Diagram

The architecture diagram shows the workflow of the application that has been created. To begin with, the user must register into the application where the user is asked to fill basic details such as username, password, email id, phone number, etc. After registration is complete, a unique PIN is sent to the respective email id of the user. Then the user can login into the application with their user name and the password. Once the user is validated, he/she is given two options for PIN entry such as SteganoPIN method and Session key method. Any one of the methods can be selected for entering the PIN. When the user's PIN is validated, the ATM transactions can be performed by the user.

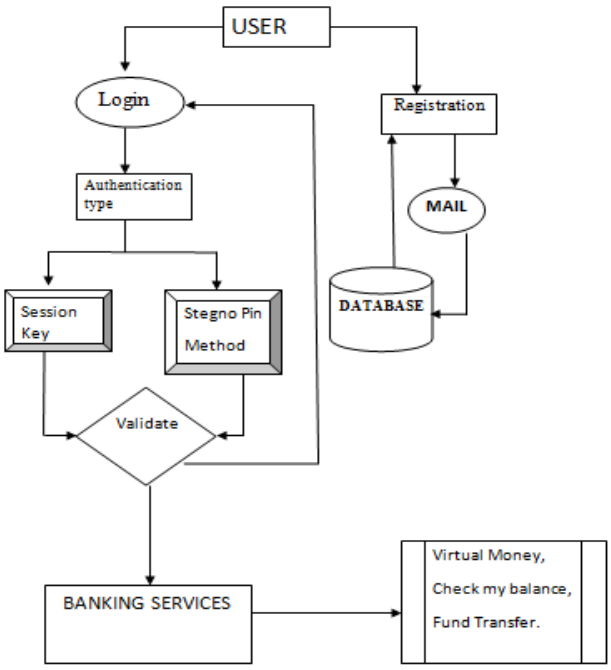


Fig.8

## 6. Conclusion

When compared with other advanced PIN entry systems, SteganoPIN is at the top of the ladder as its PIN entry time is much faster and the rate of error occurrence is relatively low. Ease of use and enhanced security is also guaranteed in our PIN entry method. Through thorough analysis it can be concluded that the SteganoPIN is resistant against camera-based shoulder surfing attacks and guessing attacks. Assuming that the user uses the system in a proper manner, the SteganoPIN is secure even against camera-based shoulder-surfing attacks over multiple authentication sessions. The system can be operated with one hand for both PIN generation and entry which increases usability.

Interestingly, although we were originally concerned that the small size of the challenge keypad was a drawback, we came to understand that it could actually enhance security. The process of using a cupped hand posture is likely to be a disadvantage of our method when compared to the standard PIN entry method. Users who are unable to cup their hands in the posture required by the system might find this method difficult.

Cameras installed right over the user remains a concern as our method guarantees security based on a physical hand protection process. Using a method that requires a simplified hand shape can possibly reduce the security of the system. The circular touch area should be placed as close to the user as possible in order to implement our method in the desired manner. Hence, for systems such as ATM and Point of Sale (PoS) terminals our method i.e., the SteganoPIN system is more effective compared to other systems. However, it can still be useful for users who want stronger security for their mobile phones in a public place.

Session Key method uses symbols instead of actual personalized identification numbers (PINs). This method is therefore resilient to shoulder surfing attacks. Active guessing attack is also ruled out by this method. Virtual money is a promising option for users who are running short of money or do not have their credit/debit cards. Thus, both SteganoPIN and Session key methods can be used to increase security wherever PIN based authentication is needed.

## References

[1] Taekyoung Kwon and Sarang Na, SteganoPIN: Two-Faced Human–Machine Interface for Practical Enforcement of PIN Entry Security, IEEE Transactions On Human-Machine Systems, Vol. 46, No. 1, February 2016.

[2] Kavitha V, Dr. G. Umarani Srikanth, Moving ATM Applications to Smart phones with a Secured Pin Entry Methods, IOSR Journal of Computer Engineering (IOSR-JCE), 17(1), Ver. II, Jan – Feb. 2015.

[3] J. Long and J. Wiles, No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Boston, MA, USA: Syngress, 2008.

[4] A. Greenberg. (2014, Jun.). Google glass snoopers can steal your passcode with a glance," Wired. [Online]. Available: http://www.wired.com/2014/06/google-glass-snoopers-can-steal-your-passcode-with-a-glance/

[5] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in Proc.ACMComput.Commun. Security, 2004,pp. 236–245.

[6] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," IEEE Trans. Syst., Man,Cybern., Syst., vol. 44, no. 6, pp. 716–727, Jun. 2014.

[7] Q. Yan, J. Han, Y. Li, and R. H. Deng, "On limitations of designing leakage-resilient password systems: Attacks, principles and usability,"in Proc. 19th Internet Soc. Netw. Distrib. Syst. Security Symp, 2012, pp. 1–16.

[8] A. Parti and F. Z. Qureshi, "Integrating consumer smart cameras into camera networks: Opportunities and obstacles," IEEE Comput., vol. 47, no. 5, pp. 45–51, May 2014.